In The United States Patent and Trademark Office
Before The Board of Patent Appeals and Interferences

In re Patent Application of:	Graunke, *et al.*	Examiner:	Gurshman, G.
		Art Unit:	2132
Application No.:	09/385,589		
Filed:	August 29, 1999		
For:	A STREAM CIPHER HAVING A SHUFFLE NETWORK COMBINER FUNCTION		

APPEAL BRIEF
IN SUPPORT OF APPELLANTS' APPEAL
TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

Honorable Commissioner of
Patents and Trademarks
Washington, D.C. 20231

Sir/Madam:

Appellants (hereafter "Appellants") hereby submit this Brief in triplicate in support of his Appeal from a final decision by the Examiner in the above-captioned case. Appellants respectfully request consideration of this Appeal by the Board of Patent Appeals and Interferences for allowance of the claims in the above-captioned patent application.

An oral hearing is not desired.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The invention is assigned to Intel Corporation of 2200 Mission College Boulevard, Santa Clara, California 95052.

II. RELATED APPEALS AND INTERFERENCES

To the best of Appellants' knowledge, there are no appeals or interferences related to the present appeal, which will directly affect, be directly affected by, or have a bearing on the Board's decision.

III. STATUS OF THE CLAIMS

Claims 1-15, and 17-30 remain in the above-referenced patent application and are the subject of the present appeal. In a Final Office Action mailed on December 30, 2003, the status of the claims is as follows:

- claims 1-15 and 28-30 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Wasilewski *et al.* (hereinafter 'Wasilewski;' US Patent No. 5,341,425) in combination with Richard *et al.* (hereinafter 'Richard;' US Patent No. 4,004,089);
- and claims 17-27 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Shukla (US Patent No. 6,345,101 B1) in combination with Richard.

Claim 16 was withdrawn from consideration during the prosecution of the present application.

IV. STATUS OF THE AMENDMENTS

In response to the Office Action mailed on December 30, 2003, in which claims 1-15, and 17-30 were rejected, or objected to, Appellants timely filed a Notice of Appeal on March 04, 2004.

Claims 17-27, 29 and 30 were amended to correct an inadvertent and minor typographical error as a result of a 37 C.F.R. § 1.126 rejection in a response mailed October 29, 2003. Claim 17 was amended and claim 16 was withdrawn from consideration in the response mailed October 29, 2003.

None of these amendments were in response to the currently pending rejection(s). A copy of all claims on appeal, claims 1-15, and 17-30, is attached hereto as Appendix A.

V. SUMMARY OF THE INVENTION

Crytographic ciphers can be broadly divided into block ciphers and stream ciphers. Block ciphers cipher a block of plain text into ciphered text by applying multiple successive rounds of transformation to the plain text, using a cipher key. An example of a block cipher is the well known DES cipher. Stream ciphers cipher a stream of plain data into ciphered data by combining the stream of plain data with a pseudo random sequence dynamically generated using a cipher key. An example of a stream cipher is the well known XPF/KPD cipher.

Most stream ciphers employ one or more linear feedback shift registers (LFSR). In various applications, it is desirable to employ multiple LFSRs to increase the robustness of a stream cipher. However, employment of multiple LFSRs requires employment of a combiner function to recombine the multiple data bits output by the LFSRs. Most combiner functions

known in the art are inefficient in their real estate requirement for hardware implementations. Thus, a robust stream cipher with a more efficient combiner function is desired.

Briefly, in accordance with one embodiment of the invention, a stream cipher is provided with one or more data bit generators to generate a first, second and third set of data bits. The stream cipher is further provided with a combiner function having a network of shuffle units to combine the third set of data bits, using the first and second sets of data bits as input data bits and control signals respectively of the network of shuffle units.

Of course, the above is merely an example embodiment and the disclosed subject matter is not limited in scope to this or any particular embodiments.

VI. ISSUE PRESENTED

The first issue is whether claims 1-15 and 28-30 are unpatentable under 35 U.S.C. § 103(a) over Wasilewski in combination with Richard.

The second issue is whether claims 17-27 are unpatentable under 35 U.S.C. § 103(a) over Shukla in combination with Richard.

VII. GROUPING OF CLAIMS

For the purposes of this appeal:

- Claims 1-15 stand or fall together as Group I;
- Claims 17-27 stand or fall together as Group II; and
- Claims 28-30 stand or fall together as Group III.

Reasons for separate patentability of the above-indicated Claim Groups are presented in the argument section pursuant to 37 C.F.R § 1.192(c)(5).

VIII. ARGUMENT

THE REJECTION OF CLAIMS 1-15 AND 28-30 (GROUPS I & III) UNDER 35 U.S.C. § 103(A) OVER WASILEWSKI IN COMBINATION WITH RICHARD, AND CLAIMS 17-27 (GROUP II) UNDER 35 U.S.C. § 103(A) OVER SHUKLA IN COMBINATION WITH RICHARD IS IMPROPER. NONE OF THE CITED PATENTS, ALONE OR IN COMBINATION, EXPRESSLY NOR INHERENTLY MEET CLAIM LIMITATIONS DIRECTED TO USING THE FIRST AND SECOND PLURALITY OF DATA BITS AS FIRST INPUT DATA BITS AND CONTROL SIGNALS RESPECTIVELY OF THE NETWORK OF SHUFFLE UNITS.

A. Claim Group I: 35 U.S.C. § 103(a)

The Examiner has rejected Claim Group I, claims 1-15, under 35 U.S.C. § 103(a) over Wasilewski in combination with Richard. Appellants respectfully disagree with the Examiner's rejection and submits that the cited documents, either alone or in combination, fail to meet the legal test to be applied under this statutory provision.

M.P.E.P. § 706.02(j) sets forth the standard for a § 103(a) rejection:

> To establish a prima facie case of obviousness, three basic criteria must be met.
> First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or combine reference teachings.
> Second, there must be a reasonable expectation of success.
> Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.
> The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991) (whitespace added).

Appellants begin with claim 1. Claim 1 recites:

> 1: (Original) An apparatus comprising:
> at least one data bit generator to generate a first, second and third plurality of data bits; and
> a combiner function, coupled to the at least one data bit generator, including a network of shuffle units, to combine the third plurality of data bits, using the first and second plurality of data bits as first input data bits and control signals respectively of the network of shuffle units.

Appellants respectfully assert that the combination set forth by the Examiner fails to meet the requirement for a *prima facie* case for a § 103(a) rejection for at least the following reasons.

1. All Claim Limitations Must Be Taught Or Suggested

M.P.E.P. § 706.02(j) sets forth that the third element for the standard for a § 103(a) rejection. The third element is that the combination must include "all claim limitations" of the rejected claim. It is respectfully asserted that neither Wasilewski nor Richard, either alone or in combination, suggests or describes "**using the first and second plurality of data bits as first input data bits and control signals respectively of the network of shuffle unit.**" The Examiner asserts that the data stream 158 of Fig. 5 of Wasilewski teaches this limitation. However, it is respectfully asserted that Wasilewski does **not** teach using the outputs of encrypter 154 as **control signals** to combiner 156. Instead, Wasilewski teaches using the outputs of encrypter 154 as **data input signals** to combiner 156. Therefore, even if the combination were proper, although Appellants believe that it is not, nonetheless, the combination would still fail to produce the invention as recited in the rejected claims.

a) Wasilewski only discloses "input" bits, not "control" signals

The Office Action of December 30, 2003 (hereafter, "the December Office Action") at pages 2 and 3 cites the combiner 156 of *Wasilewski* as disclosing the limitations noted above. Specifically, the December Office Action at page 2 asserts: "[*Wasilewski*] shows in Fig. 5 that signals from encryptor is being input in combiner where it controls the process." As Appellants are able to understand this reasoning, the December Office Action is asserting that *Wasilewski*'s input signals are the same as control signals for its combiner, and that an input signals control the process of the logic block (combiner 156) to which they are input. Appellants must respectfully disagree.

Appellants first point out that *Wasilewski* is silent regarding the control and/or the functioning of its combiner 156, and merely states: "Combiner/transmitter 156 may combine the encrypted sets of data in any manner suitable for a given application. For example, combiner 156 may perform frequency-division multiplexing. Alternatively, combiner 156 may combine the encrypted data sets using a time-division multiplexing scheme." See col. 12, lines 53 to 66. Thus, *Wasilewski*'s data sets are data that is already encrypted, and is being placed in a combiner that will interleave segments of the different data sets into a single transmission stream in accordance with FDM or TDM. Appellants do not understand how *Wasilewski*'s discussion of preparing an encrypted data stream for transmission according to a transmission scheme is purported to disclose or suggest control signals to logic blocks. There is no discussion in *Wasilewski* about how the input data sets, as apparently asserted by the December Office Action, are purported to control how the different data sets are to be prepared for transmission. Thus, Appellants must respectfully submit that *Wasilewski* provides no direct support for the assertion in the December Office Action.

b) Definition of "input" bits, not "control" signals

Furthermore, Appellants next point out that the assertion in the December Office Action fails as a matter of logic. An input to a logic function does not "control the process." For example, if inputs 0 and 1 were inputs to an AND gate, the process would be the ANDing of the inputs, and the result (the outcome) would be 0. Changing the inputs to 1 and 1 would not alter the process, which would continue to be the ANDing of the inputs, even though the outcome (or "result") would change to 1. Appellants submit that this would hold true for a non-logic function, such as the combining of data sets for transmission according to TDM or FDM, as cited in the December Office Action.

Appellants respectfully point out that M.P.E.P. § 2111 states that "during patent examination, the pending claims must be given their broadest **reasonable** interpretation **consistent with the specification**," and that "the broadest reasonable interpretation of the claims must also be consistent with the interpretation that those skilled in the art would reach." Appellants again note that the claim recites both "input data bits" and "control signals" in the claims. Were these two terms interpreted to be analogous, the interpretation would render one of the terms redundant, and would fail to give meaning to the words of the claims. Therefore, it is respectfully asserted that to define the terms "input bits" and "control signals" in a fashion that would render them identical and the claim illogical is not a "reasonable interpretation." Thus, Appellants respectfully submit that the reasoning used to support the rejection of claim 1 fails as a matter of logic, and fails to find support in the cited references.

c) Richard fails to cure the deficiency of Wasilewski

Furthermore, *Richard* is cited only as disclosing a shuffle unit, and fails to cure the deficiencies of *Wasilewski* set forth above. Therefore, Appellants respectfully submit that either alone or in combination, the cited references fail to disclose or suggest every element of claim 1.

d) Conclusion

Therefore, even if the Examiner's assertion as to what Richard and Wasilewski teaches is correct, it is respectfully asserted that neither Wasilewski nor Richard, either alone or in combination, suggests or describes "**using the first and second plurality of data bits as first input data bits and control signals respectively of the network of shuffle unit.**" Therefore, even if the combination were proper, although Appellants believe it is not, nonetheless, the combination would still fail to produce the invention as recited in the rejected claim. Therefore, Appellants respectfully submits that Claim Group I recites patentable subject matter.

B. Claim Group II: 35 U.S.C. § 103(a)

The Examiner has rejected Claim Group II, claims 17-27, under 35 U.S.C. § 103(a) as being unpatentable over Shukla in combination with Richard. Appellants respectfully disagree with the Examiner's rejection and submit that the cited documents, either alone or in combination, fail to meet the legal test to be applied under this statutory provision.

Appellants begin with claim 17. Claim 17 recites:

> 17: (Previously Presented) An apparatus comprising:
> a first XOR gate to receive a first plurality of data bits and combine them into a second data bit;
> a network of shuffle units, coupled to the first XOR gate, to output a third data bit by shuffling and propagating the second data bit through the network of shuffle units under the control of a fourth plurality of data bits; and
> a second XOR gate coupled to the network of shuffle units to combine a fifth plurality of data bits using the third data bit;
> wherein at least one of the shuffle units comprises a first and a second flip-flop to store a first and a second state value, and a plurality of selectors coupled to the first and second flip-flops to control selective output of one of the first and second state values based on a corresponding one of said fourth plurality of data bits.

Appellants respectfully assert that the combination set forth by the Examiner fails to meet the requirement for a *prima facie* case for a § 103(a) rejection, cited above in reference to Claim Group I, for at least the following reasons.

1. All Claim Limitations Must Be Taught Or Suggested

M.P.E.P. § 706.02(j) sets forth that the third element for the standard for a § 103(a) rejection. The third element is that the combination must include "all claim limitations" of the rejected claim. It is respectfully asserted that neither Shukla nor Richard, either alone or in combination, suggests or describes "**a plurality of selectors ... to control selective output ... based on a corresponding one of said fourth plurality of data bits**."

a) December Office Action silent on specific grounds for rejection

Appellants respectfully point out that the Office Action of December 30, 2003 fails to discuss the limitations of the claim highlighted below.

17: (Previously Presented) An apparatus comprising:

a first XOR gate to receive a first plurality of data bits and combine them into a second data bit;

a network of shuffle units, coupled to the first XOR gate, to output a third data bit by shuffling and propagating the second data bit through the network of shuffle units **under the control of a fourth plurality of data bits**; and

a second XOR gate coupled to the network of shuffle units to combine a fifth plurality of data bits using the third data bit;

wherein at least one of the shuffle units comprises a first and a second flip-flop to store a first and a second state value, and **a plurality of selectors coupled to the first and second flip-flops to control selective output of one of the first and second state values based on a corresponding one of said fourth plurality of data bits**.

The bare assertion in the December Office Action on page 5 that "*Shukla* explicitly shows the limitations, recited in the independent claim 17, in Fig. 3" fails to point out what in *Shukla* is purported to show, explicitly or otherwise, the limitations recited in claim 17. Appellants note that Fig. 3 of *Shukla* merely shows a block diagram with blocks consisting of: a plaintext starting point, and encryption rounds having an XOR1 operation, a shuffle operation, and an XOR 2 operation. Fig. 3 fails to explicitly show either the control of the XOR operations, or a plurality of selectors as recited in the claims. Nor has the December Office Action pointed to anything in Fig. 3 or any of the text of *Shukla* that is purported to disclose or suggest these elements of the claimed invention. Nor has the December Office Action provided any reasoning to suggest how *Shukla* may be interpreted as disclosing these items.

Furthermore, the December Office Action cites *Richard* only as disclosing a shuffle unit, and fails to point to anything in *Richard* that is purported to disclose or suggest the limitations discussed above. Therefore, Appellants must submit that the December Office Action has failed to provide a complete rejection of claim 17.

b) Shukla and Richard fail to teach all limitations

In the December Office Action, on page 2, the Examiner states "Applicant's arguments with respect to claims 17-30 (*sic*) have been considered but are moot in view of the new ground(s) of rejection." However, both the December Office Action and the Office Action dated May 06, 2003 (hereafter, "the May Office Action") reject claims 17-27 based upon Shukla in combination with Richard. Appellants respectfully fail to understand "the new grounds" the Examiner cites.

It is respectfully asserted that neither Shukla nor Richard, either alone or in combination, suggests or describes "**a plurality of selectors ... to control selective output ... based on a corresponding one of said fourth plurality of data bits**." The PTO, in the May Office Action, asserts that the selectors attached to elements 70, 71, 75, 72 of Fig. 2A of Richard teaches this limitation. However, it is respectfully asserted that Richard does **not** teach using the selectors **controlled by "said fourth plurality of data bits."** As an illustrative embodiment of Appellants disclosed subject matter, see page 14, lines 5 and 6, "[e]ach selector 814a, 814b, or 814c receives a corresponding one of the second group of LFSR outputs as a control signal." Instead, Richard teaches using the selectors **controlled by a decrypt or encrypt bit**. The December Office Action was silent on this point, as discussed above.

As mentioned above, the December Office Action cites *Richard* only as disclosing a shuffle unit, and fails to point to anything in *Richard* that is purported to disclose or suggest the limitations discussed above.

Therefore, even if the combination were proper, although Appellants believe that it is not, nonetheless, the combination would still fail to produce the invention as recited in the rejected claims. It is, therefore, respectfully requested that the rejection of this claim be withdrawn.

c) Conclusion

Therefore, even if the Examiner's assertion as to what Shukla and Richard teaches is correct, it is respectfully asserted that neither Shukla nor Richard, either alone or in combination, suggests or describes ""**a plurality of selectors ... to control selective output ... based on a corresponding one of said fourth plurality of data bits**." Therefore, even if the combination were proper, although Appellants believe it is not, nonetheless, the combination would still fail to produce the invention as recited in the rejected claim. Therefore, Appellants respectfully submit that Claim Group II recites patentable subject matter.

RECEIVED
SEP 17 2004
Technology Center 2100

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application No.	09/385,589
Filing Date	August 29, 1999
First Named Inventor	Gary L. Graunke
Art Unit	2132
Examiner Name	Grigory Gurshman
Total Number of Pages in This Submission	Attorney Docket Number: 42390P7574

ENCLOSURES *(check all that apply)*

- [X] Fee Transmittal Form
  - [X] Fee Attached
- [ ] Amendment / Response
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [X] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
  - [ ] PTO/SB/08
- [ ] Certified Copy of Priority Document(s)
- [ ] Response to Missing Parts/ Incomplete Application
  - [ ] Basic Filing Fee
  - [ ] Declaration/POA
  - [ ] Response to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert a Provisional Application
- [ ] Power of Attorney; Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s)
- [ ] After Allowance Communication to Group
- [ ] Appeal Communication to Board of Appeals and Interferences
- [X] Appeal Communication to Group **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [X] Other Enclosure(s) *(please identify below):*
  - Check for $330.00
  - Check for $2010.00
  - Return Receipt Postcard

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Gregory D. Caldwell, Reg. No. 39,926 BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Signature	
Date	September 10, 2004

CERTIFICATE OF MAILING/TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Typed or printed name	**Tamara M. Simpson**		
Signature		Date	**September 13, 2004**

RECEIVED
SEP 17 2004
Technology Center 2100

FEE TRANSMITTAL for FY 2004

Effective 01/01/2004. Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27.

TOTAL AMOUNT OF PAYMENT ($) 2,340.00

Complete if Known	
Application Number	09/385,589
Filing Date	August 29, 1999
First Named Inventor	Gary L. Graunke
Examiner Name	Grigory Gurshman
Art Unit	2132
Attorney Docket No.	42390P7574

METHOD OF PAYMENT *(check all that apply)*

☒ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☐ Deposit Account

Deposit Account Number: 02-2666

Deposit Account Name: Blakely, Sokoloff, Taylor & Zafman LLP

The Commissioner is authorized to: *(check all that apply)*

☐ Charge fee(s) indicated below ☒ Credit any overpayments

☒ Charge any additional fee(s) or underpayment of fees as required under 37 CFR §§ 1.16, 1.17, 1.18 and 1.20.

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	770	2001	385	Utility filing fee	
1002	340	2002	170	Design filing fee	
1003	530	2003	265	Plant filing fee	
1004	770	2004	385	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	

SUBTOTAL (1) ($)

2. EXTRA CLAIM FEES

	Extra Claims		Fee from below	Fee Paid
Total Claims	- -	- 29** =		
Independent Claims		- 3 =	X	=
Multiple Dependent			X	=

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	86	2201	43	Independent claims in excess of 3
1203	290	2203	145	Multiple Dependent claim, if not paid
1204	86	2204	43	**Reissue independent claims over original patent
1205	18	2205	9	**Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($)

***or number previously paid, if greater, For Reissues, see below*

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet.	
2053	130	2053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	420	2252	210	Extension for reply within second month	
1253	950	2253	475	Extension for reply within third month	
1254	1,480	2254	740	Extension for reply within fourth month	
1255	2,010	2255	1,005	Extension for reply within fifth month	2,010.00
1404	330	2401	165	Notice of Appeal	
1402	330	2402	165	Filing a brief in support of an appeal	330.00
1403	290	2403	145	Request for oral hearing	
1451	1,510	2451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,330	2453	665	Petition to revive - unintentional	
1501	1,330	2501	665	Utility issue fee (or reissue)	
1502	480	2502	240	Design issue fee	
1503	640	2503	320	Plant issue fee	
1460	130	2460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	770	1809	385	Filing a submission after final rejection (37 CFR § 1.129(a))	
1810	770	2810	385	For each additional invention to be examined (37 CFR § 1.129(b))	
1801	770	2801	385	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	
Other fee (specify)					

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) 2,340.00

SUBMITTED BY

Complete (if applicable)

Name (Print/Type)	Gregory D. Caldwell	Registration No. (Attorney/Agent)	39,926	Telephone	(503) 439-8778
Signature				Date	09/13/04

Based on PTO/SB/17 (10-03) as modified by Blakely, Sokoloff, Taylor & Zafman (wh) 02/10/2004.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

RECEIVED
SEP 17 2004
Technology Center 2100

FEE TRANSMITTAL for FY 2004

Effective 01/01/2004. Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27.

TOTAL AMOUNT OF PAYMENT ($) 2,340.00

Complete if Known	
Application Number	09/385,589
Filing Date	August 29, 1999
First Named Inventor	Gary L. Graunke
Examiner Name	Grigory Gurshman
Art Unit	2132
Attorney Docket No.	42390P7574

METHOD OF PAYMENT *(check all that apply)*

☒ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☐ Deposit Account

Deposit Account Number: 02-2666

Deposit Account Name: Blakely, Sokoloff, Taylor & Zafman LLP

The Commissioner is authorized to: *(check all that apply)*

☐ Charge fee(s) indicated below ☒ Credit any overpayments

☒ Charge any additional fee(s) or underpayment of fees as required under 37 CFR §§ 1.16, 1.17, 1.18 and 1.20.

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	770	2001	385	Utility filing fee	
1002	340	2002	170	Design filing fee	
1003	530	2003	265	Plant filing fee	
1004	770	2004	385	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	

SUBTOTAL (1) ($)

2. EXTRA CLAIM FEES

		Extra Claims		Fee from below		Fee Paid
Total Claims	- 29** =		X		=	
Independent Claims	- 3 =		X		=	
Multiple Dependent					=	

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	86	2201	43	Independent claims in excess of 3
1203	290	2203	145	Multiple Dependent claim, if not paid
1204	86	2204	43	**Reissue independent claims over original patent
1205	18	2205	9	**Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($)

***or number previously paid, if greater, For Reissues, see below*

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet.	
2053	130	2053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	420	2252	210	Extension for reply within second month	
1253	950	2253	475	Extension for reply within third month	
1254	1,480	2254	740	Extension for reply within fourth month	
1255	2,010	2255	1,005	Extension for reply within fifth month	2,010.00
1404	330	2401	165	Notice of Appeal	
1402	330	2402	165	Filing a brief in support of an appeal	330.00
1403	290	2403	145	Request for oral hearing	
1451	1,510	2451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,330	2453	665	Petition to revive - unintentional	
1501	1,330	2501	665	Utility issue fee (or reissue)	
1502	480	2502	240	Design issue fee	
1503	640	2503	320	Plant issue fee	
1460	130	2460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	770	1809	385	Filing a submission after final rejection (37 CFR § 1.129(a))	
1810	770	2810	385	For each additional invention to be examined (37 CFR § 1.129(b))	
1801	770	2801	385	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	
Other fee (specify)					

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) 2,340.00

SUBMITTED BY

Complete (if applicable)

Name (Print/Type)	Gregory D. Caldwell	Registration No. (Attorney/Agent)	39,926	Telephone	(503) 439-8778
Signature				Date	09/13/04

Based on PTO/SB/17 (10-03) as modified by Blakely, Sokoloff, Taylor & Zafman (wlr) 02/10/2004.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

C. Claim Group III: 35 U.S.C. § 103(a)

The Examiner has rejected Claim Group III, claims 28-30, under 35 U.S.C. § 103(a) over Wasilewski in combination with Richard. Appellants respectfully disagree with the Examiner's rejection and submit that the cited documents, either alone or in combination, fail to meet the legal test to be applied under this statutory provision.

Appellants begin with claim 28. Claim 28 recites:

> 28: (Original) A method comprising:
> generating a first, second and third plurality of data bits; and
> shuffling and propagating a fourth data bit generated from the first plurality of data bits, under the control of the second plurality of data bits, to output a fifth data bit to combine the third plurality of data bits.

Appellants respectfully assert that the combination set forth by the Examiner fails to meet the requirement for a *prima facie* case for a § 103(a) rejection, cited above in reference to Claim Group I, for at least the following reasons.

1. All Claim Limitations Must Be Taught Or Suggested

M.P.E.P. § 706.02(j) sets forth that the third element for the standard for a § 103(a) rejection. The third element is that the combination must include "all claim limitations" of the rejected claim. It is respectfully asserted that neither Wasilewski nor Richard, either alone or in combination, suggests or describes "**shuffling and propagating a fourth data bit generated from the first plurality of data bits, under the control of the second plurality of data bits**."

a) Arguments cited in Group I are incorporated by reference

Appellants note that the limitations of these claims were not directly addressed in the December Office Action (hereafter, "the Office Action"), but were merely rejected under the same rejection of claims 1-15, discussed above in Group I. To the extent that the Office Action is attempting to extend to the limitations of this claim the above-referenced assertion that input data bits are control bits, Appellants refer to the above discussion of how the assertion in the Office Action fails for both reasons of logic and lack of support in the cited references. The arguments of Group I are incorporated by reference in this subsection of the Appeal Brief.

b) Richard merely provides fixed, hardwired shuffling

Furthermore, to the extent that either *Wasilewski* or *Richard* discuss controlling shuffling, Appellants note that *Richard* at col. 6, lines 49 to 51 states: "The position of 56 jumper wires in the mating plug determines the bit interchange," thus implying that the process is controlled by **hard-wiring the hardware**. Thus, Appellants respectfully submit that the cited references, either alone or in combination, fail to disclose or suggest at least **shuffling under the control of a second plurality of data bits**, as recited in the claim. Therefore, Appellants submit that claim 28, and its dependent claims 29 & 30, are not rendered obvious by the cited references. Therefore, Appellants respectfully submit that Claim Group III recites patentable subject matter.

c) Conclusion

Therefore, even if the Examiner's assertion as to what Richard and Wasilewski teaches is correct, it is respectfully asserted that neither Wasilewski nor Richard, either alone or in

combination, suggests or describes "**shuffling and propagating a fourth data bit generated from the first plurality of data bits, under the control of the second plurality of data bits**." Therefore, even if the combination were proper, although Appellants believe it is not, nonetheless, the combination would still fail to produce the invention as recited in the rejected claim. Therefore, Appellants respectfully submits that Claim Group III recites patentable subject matter.

IX. CONCLUSION

Appellants respectfully submit that all the pending claims in this patent application are patentable and request that the Board of Patent Appeals and Interferences overrule the Examiner and direct allowance of the rejected claims.

This brief is submitted in triplicate, along with a check for the proper amount to cover the appeal fee for one other than a small entity as specified in 37 C.F.R § 1.17(c).

Respectfully submitted,

Justin B. Scout
Attorney for Appellants
Reg. No. 54,431

Dated:

Fri Sep 10, 2004

c/o Blakely, Sokoloff, Taylor & Zafman, LLP
12400 Wilshire Blvd., Seventh Floor
Los Angeles, CA 90025-1026
(503) 264-0967

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313 on:

9/13/04
Date of Deposit

Tamara Simpson
Name of Person Mailing Correspondence

Tamara Simpson 9/13/04
Signature Date

APPENDIX A: CLAIMS ON APPEAL

1. (Original) An apparatus comprising:

at least one data bit generator to generate a first, second and third plurality of data bits; and

a combiner function, coupled to the at least one data bit generator, including a network of shuffle units, to combine the third plurality of data bits, using the first and second plurality of data bits as first input data bits and control signals respectively of the network of shuffle units.

2. (Original) The apparatus of claim 1, wherein at least one of the shuffle units comprises a first and a second flip-flop to store a first and a second state value, and a plurality of selectors coupled to the first and second flip-flops in a topological manner to control selective output of one of the first and second state values based on a corresponding one of said second plurality of data bits.

3. (Original) The apparatus of claim 2, wherein said plurality of selectors are coupled to said first and second flip-flops of the shuffle unit in a topological manner that results in the first state value of the shuffle unit being output when the corresponding one of said second plurality of data bits is in a first state, and the second state value of the shuffle unit being output when the corresponding one of said second plurality of data bits is in a second state.

4. (Original) The apparatus of claim 2, wherein said plurality of the selectors are further coupled to said first and second flip-flops of the shuffle unit to control selective modification of

the first and second state values stored in said first and second flip-flops of the shuffle unit based on the same corresponding one of said second plurality of data bits.

5. (Original) The apparatus of claim 4, wherein said plurality of selectors are coupled to said first and second flip-flops of the shuffle unit in a topological manner that results in the first state value being output and the first and second flip-flops of the shuffle unit to store said second state value and a second input data bit respectively when the corresponding one of said second plurality of data bits is in a first state, and the second state value being output and the first and second flip-flops of the shuffle unit to store the second input data bit and said first state value respectively when the corresponding one of said second plurality of data bits is in a second state.

6. (Original) The apparatus of claim 5, wherein the second input value is a selected one of an output data bit of an immediately preceding shuffle unit and an output data bit generated from said first plurality of data bits.

7. (Original) The apparatus of claim 1, wherein at least one of the shuffle units comprises a first and a second flip-flop to store a first and a second state value, and a plurality of selectors coupled to the first and second flip-flops to control modification of the first and second state values based on a corresponding one of said second plurality of data bits.

8. (Original) The apparatus of claim 7, wherein said plurality of selectors are coupled to the first and second flip-flops in a topological manner that results in the first and second flip-flops of the shuffle unit to store said second state value and a second input data bit respectively when the

corresponding one of said second plurality of data bits is in a first state, and the first and second flip-flops of the shuffle unit to store the second input data bit and said first state value respectively when the corresponding one of said second plurality of data bits is in a second state.

9. (Original) The apparatus of claim 8, wherein the shuffle units are serially coupled to each other with a first of the shuffle unit serially coupled to the first XOR gate, and said second input data bit is a selected one of an output bit of an immediately preceding shuffle unit and an output bit generated from the first plurality of data bits.

10. (Original) The apparatus of claim 1, wherein the combiner function further comprises an exclusive-OR gate to combine the first plurality of data bits for the network of shuffle units.

11. (Original) The apparatus of claim 1, wherein the combiner function further comprises an exclusive-OR gate to combine the third plurality of data bits using an output bit of the network of shuffle units.

12. (Original) The apparatus of claim 11, wherein the apparatus further comprises a register coupled to the XOR gate to store a cipher key and allow the stored cipher key to be periodically modified by the output of the exclusive-OR gate.

13. (Original) The apparatus of claim 12, wherein the apparatus further comprises a function block coupled to the register to successively transform the modified cipher key, and a mapping

block coupled to the register to generate a pseudo random bit sequence based on the successive transformed states of the modified random number.

14. (Original) The apparatus of claim 1, wherein the at least one data bit generator comprises a plurality of LFSRs to generate said first, second, and third plurality of data bits.

15. (Original) The apparatus of claim 1, wherein the apparatus is a stream cipher.

16. (Cancelled).

17. (Previously Presented) An apparatus comprising:

a first XOR gate to receive a first plurality of data bits and combine them into a second data bit;

a network of shuffle units, coupled to the first XOR gate, to output a third data bit by shuffling and propagating the second data bit through the network of shuffle units under the control of a fourth plurality of data bits; and

a second XOR gate coupled to the network of shuffle units to combine a fifth plurality of data bits using the third data bit;

wherein at least one of the shuffle units comprises a first and a second flip-flop to store a first and a second state value, and a plurality of selectors coupled to the first and second flip-flops to control selective output of one of the first and second state values based on a corresponding one of said fourth plurality of data bits.

18. (Previously Presented) The apparatus of claim 17, wherein said plurality of selectors are coupled to the first and second flip-flops of the shuffle unit in a topological manner that results in the first state value of the shuffle unit being output when the corresponding one of said fourth plurality of data bits is in a first state, and the second state value of the shuffle unit being output when the corresponding one of said fourth plurality of data bits is in a second state.

19. (Previously Presented) The apparatus of claim 18, wherein said plurality of the selectors are further coupled to the first and second flip-flops to control selective modification of the first and second state values stored in the first and second flip-flops of the shuffle unit based on the same corresponding one of said fourth plurality of data bits.

20. (Previously Presented) The apparatus of claim 19, wherein said plurality of selectors are coupled to the first and second flip-flops of the shuffle unit in a topological manner that results in the first state value being output and the first and second flip-flops of the shuffle unit to store said second state value and a sixth data bit respectively when the corresponding one of said fourth plurality of data bits is in a first state, and the second state value being output and the first and second flip-flops of the shuffle unit to store the sixth data bit and said first state value respectively when the corresponding one of said fourth plurality of data bits is in a second state.

21. (Previously Presented) The apparatus of claim 20, wherein the shuffle units are serially coupled to each other with a first of the shuffle unit serially coupled to the first XOR gate, and said sixth data bit is a selected one of said second data bit and the output of an immediately preceding shuffle unit.

22. (Previously Presented) The apparatus of claim 17, wherein at least one of the shuffle units comprises a first and a second flip-flop to store a first and a second state value, and a plurality of selectors coupled to the first and second flip-flops to control modification of the first and second state values based on a corresponding one of said fourth plurality of data bits.

23. (Previously Presented) The apparatus of claim 22, wherein said plurality of selectors are coupled to the first and second flip-flops of the shuffle unit in a topological manner that results in the first and second flip-flops of the shuffle unit to store said second state value and a sixth data bit respectively when the corresponding one of said fourth plurality of data bits is in a first state, and the first and second flip-flops of the shuffle unit to store the sixth data bit and said first state value respectively when the corresponding one of said fourth plurality of data bits is in a second state.

24. (Previously Presented) The apparatus of claim 23, wherein the shuffle units are serially coupled to each other with a first of the shuffle unit serially coupled to the first XOR gate, and said sixth data bit is a selected one of said second data bit and the output of an immediately preceding shuffle unit.

25. (Previously Presented) The apparatus of claim 17, wherein the apparatus further comprises a register coupled to the second exclusive-OR gate to store a value to be periodically modified using the result of said combination of the fifth plurality of data bits.

26. (Previously Presented) The apparatus of claim 25, wherein the apparatus further comprises a function block coupled to the register to successively transform a modified version of the stored value, and a mapping block coupled to register to generate a pseudo random bit sequence based on the successively transformed states of the modified value.

27. (Previously Presented) The apparatus of claim 26, wherein the apparatus is a stream cipher.

28. (Original) A method comprising:

generating a first, second and third plurality of data bits; and

shuffling and propagating a fourth data bit generated from the first plurality of data bits, under the control of the second plurality of data bits, to output a fifth data bit to combine the third plurality of data bits.

29. (Previously Presented) The method of claim 28, wherein the fourth data bit is serially shuffle and propagated, and at each stage, a first state value is output when the corresponding one of said second plurality of data bits is in a first state, and a second state value is output when the corresponding one of said second plurality of data bits is in a second state.

30. (Previously Presented) The method of claim 28, wherein the fourth data bit is serially shuffle and propagated, and at each stage, a first of the state values is replaced by an input value, and shuffled, when the corresponding one of said second plurality of data bits is in a first state,

and a second of the state values is replaced by the input value, and shuffled, when the corresponding one of said second plurality of data bits is in a second state.